(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 115 242 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
11.07.2001 Patentblatt 2001/28

(51) Int Cl.[7]: **H04M 3/38**, H04L 29/06, G06F 1/00

(21) Anmeldenummer: **00810008.3**

(22) Anmeldetag: **06.01.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(71) Anmelder: **Swisscom AG**
3000 Bern 29 (CH)

(72) Erfinder:
- **Eberhardt, Rolf**
  3075 Rüfenacht (CH)
- **Lehmann, Lorenz**
  3122 Kehrsatz (CH)

(74) Vertreter: **BOVARD AG - Patentanwälte**
Optingenstrasse 16
3000 Bern 25 (CH)

(54) Authentifikation eine Abonnenten eines Telekommunikationsdienstes mittels einer häufig gewählten Zieladresse

(57) Verfahren und System zur Authentifikation eines Abonnenten eines Telekommunikationsnetzes, dadurch gekennzeichnet, dass der Abonnent (10) mindestens eine der über eine Abonnentenadresse des Telekommunikationsnetzes häufig gewählten Zieladresse einem Authentifikationssystem (20) angibt, und dass das Authentifikationssystem (20) die angegebene Zieladresse mit häufig gewählten Zieladressen vergleicht, die der Abonnentenadresse zugeordnet und abgespeichert (42) sind. Ein Servermodul (30) beinhaltet dabei sowohl die Schnittstelle zum Abonnenten (10) als auch gleichzeitig den möglichen Dienst eines Anbieters. Das Servermodul (30) kann über eine Authentifizierungseinheit (40) mit Schnittstelle (45) den Abonnenten (10) authentifizieren lassen. Dies kann entweder über ein Auswahlverfahren oder über die direkte Angabe einer häufig gewählten Zieladresse einer Abonnentenadresse geschehen. Der Abonnent (10) kann insbesondere Benutzer eines Telefonnetzes oder eines IP-Netzes sein.

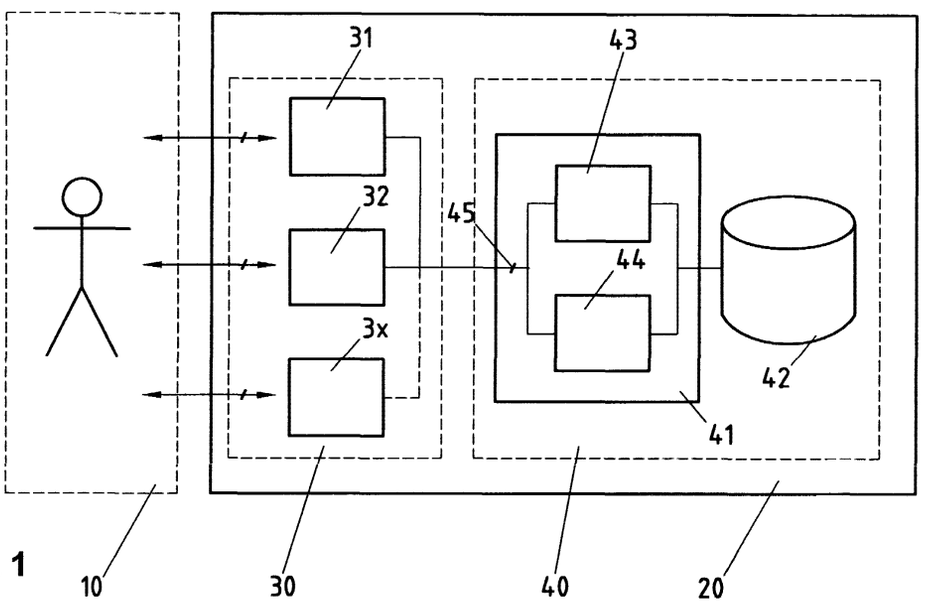

FIG. 1

EP 1 115 242 A1

Beschreibung

[0001] Die vorliegende Erfindung beschreibt ein Verfahren zur Authentifikation von Abonnenten von Telekommunikationsdiensten. Die Erfindung betrifft insbesondere die Authentifikation von Telefonnetz- und IP-Netzbenutzern, welche von Internetdiensten und/oder Telekommunikationsdiensten Gebrauch machen.

[0002] Eine grosse Bandbreite von verschiedenen Kundendiensten wird heute über Telekommunikationsnetze, insbesondere das Internet, das öffentliche geschaltete Telefonnetz und/oder Mobilfunknetze, angeboten. Beispiele dafür sind das Bestellen von Waren übers Internet, das elektronische Bezahlen von Waren oder das Abfragen von Datenbanken (Kontostand, Börsenkurse etc.), beispielsweise via SMS (Short Message Services), IVR (Interactive Voice Response) oder Web-Interface. Durch diese Entwicklung entsteht ein wachsendes Bedürfnis von Seiten der Anbieter und Kunden nach möglichst grosser Sicherheit bezüglich Authentizität, das heisst der gesicherten Identität des Kunden, welcher den Service in Anspruch nimmt. Bei der Authentifikation werden häufig Personal Identification Numbers (PIN) und/oder sogenannte Smartcards verwendet. Smartcards setzen jedoch ein Kartenlesegerät voraus. In beiden Fällen wird der Name oder eine andere Identifikation des Kunden sowie die PIN zum Remote-Server des Dienst- oder Produkteanbieters übermittelt. Ein Authentifikationssystem entschlüsselt (falls notwendig) und überprüft die PIN über eine entsprechende Datenbank und authentifiziert den Kunden. Kreditkarten bilden eine Ausnahme. Benutzt der Kunde seine Kreditkarte an einer Cash-Station, gibt er seine PIN ein. Typischerweise enthält der Magnetstreifen der Kreditkarte die Kontonummer und die verschlüsselte PIN des autorisierten Inhabers, die Entschlüsselung erfolgt jedoch im Kartenlesegerät selbst. Da der Magnetstreifen die PIN enthält und der Besitzer eines Kartenlesegeräts und des entsprechenden Dekodiergerätes über die Möglichkeit verfügt, die PIN zu entschlüsseln, bietet die Eingabe einer PIN bei Kreditkarten nicht notwendigerweise einen effektiven Schutz. Smartcards versuchen dieses Problem durch eine zusätzliche Verschlüsselung der PIN zu lösen. Dies geschieht entweder durch einen dynamischen Zahlenschlüssel, welcher z.B. Zeit, Tag oder Monat enthält oder einen anderen Algorithmus. Die Entschlüsselung und Authentifikation geschieht aber nicht im Gerät selbst, sondern extern über ein Authentifikationssystem. Dies ergibt eine zusätzliche Sicherheit.

[0003] Es ist eine Aufgabe der Erfindung, ein neues Verfahren und System zur Authentifikation eines Abonnenten eines Telekommunikationsnetzes, insbesondere des öffentlich geschalteten Telefonnetzes, eines ISDN-Netzes, eines Mobilfunknetzes und/oder eines IP-Netzes, vorzuschlagen, welche beispielsweise ermöglichen, den Abonnenten bei der Verwendung von Telekommunikationsdiensten zu authentifizieren, ohne dabei Smartcards und dafür erforderliche Kartenlesegeräte oder PINs zu verwenden.

[0004] Gemäss der vorliegenden Erfindung wird dieses Ziel insbesondere durch die Merkmale der unabhängigen Ansprüche erreicht. Weitere vorteilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

[0005] Insbesondere werden diese Ziele durch die Erfindung dadurch erreicht, dass der Abonnent eines Telekommunikationsnetzes einem Authentifikationssystem mindestens eine der über eine Abonnentenadresse des Telekommunikationsnetzes am häufigsten gewählten Zieladressen angibt und das Authentifikationssystem die angegebene Zieladresse mit häufig gewählten Zieladressen vergleicht, die der Abonnentenadresse zugeordnet und in einer Datenbank abgespeichert sind. Als Ausführungsvarianten kann der Abonnent insbesondere ein Abonnent eines Telefonnetzes oder der Benutzer eines IP-Netzes sein. Die Abonnentenadresse kann beispielsweise eine Anschlussnummer eines Telefonnetzes oder eine IP-Nummer eines IP-Netzes sein und die häufig gewählten Zieladressen entsprechend häufig gewählte Telefonnummern oder IP-Nummern. Bei IP-Netzen können statt den IP-Nummern auch die URL (Universal Resource Locator) für die Zieladressen und/oder Abonnentenadressen zur Authentifizierung verwendet werden. Beim Abonnenten kann es sich typischerweise um ein Benutzer von Telekommunikationsdiensten, wie Internetshopping, elektronische Zahlungsverfahren oder Telebanking, handeln, welcher über eine Abonnentenadresse in einem Telekommunikationsnetz verfügt. Das Telekommunikationsnetz kann wie oben beschrieben, insbesondere ein öffentlich geschaltetes Telefonnetz, ein ISDN-Netz, ein Mobilfunknetz und/oder ein IP-Netz sein. Dabei ist die Schnittstelle zum Abonnenten beispielsweise eine graphische Schnittstelle GUI, wie bei Web-Interfaces, oder eine Interactive Voice Responce IVR-Schnittstelle. Es ist darauf hinzuweisen, dass die Verbindung vom Abonnenten zum Authentifikationssystem zumindest zum Teil über ein Mobilfunknetz, z.B. ein GSM- oder UMTS-Netz, und/oder ein oder mehrere Festnetze, insbesondere das Internet und das öffentliche Telefonnetz, erfolgen kann. Zur Übermittlung bei Mobilfunknetzen können verschiedene Übermittlungsstandards wie SMS (Short Message System) oder USSD (Unstructured Supplementary Service Data) verwendet werden. Dazu gehört auch WAP (Wireless Application Protocoll) zum Benutzen von Web-Diensten übers Mobilfunknetz oder GPRS (Generalized Packet Radio Service). Um den Sicherheitsstandard bei der Übermittlung zu erhöhen, kann die ausgetauschte Information zusätzlich verschlüsselt werden durch feste, dynamische, symmetrische, asymmetrische oder andere Verschlüsselungsalgorithmen. Die Erfindung kann auch als zusätzliches Authentifikationssystem oder Ergänzung zu anderen Authentifikationssystemen dienen, z.B. als zusätzliche Sicherheitsprüfung bevor einem Kunden eine PIN generiert wird. Die

Anwendung des Authentifikationsverfahrens und -systems ist nicht auf Telekommunikationsdienste beschränkt.

[0006] Die Information zur Authentifikation des Abonnenten (z.B. des Internet-Kunden) sollte für Dritte nicht leicht zu fälschen sein, so dass der Anbieter eines Dienstes sicher sein kann, mit der tatsächlich autorisierten Person verbunden zu sein. Einer der Vorteile der Erfindung ist, dass z.B. bei Telefonnetzen die durch den Abonnenten unter einem bestimmten Telefonanschluss gewählten Telefonnummern eine solche geeignete Information darstellen, da es u.a. durch die hohe Sicherheit in Telefonnetzen möglichen Betrügern schwierig gemacht ist, den Telefonverkehr eines Kunden zu kontrollieren. Die Einfachheit des Authentifikationsverfahrens und -Systems für den Abonnenten ist ein weiterer Vorteil der Erfindung. So werden zur Identifizierung weder feste PINs oder Passwörter, noch Smartcards oder SIM-Karten (Subscriber Identity Module) verwendet, mit ihren eingangs besprochenen Nachteilen bezüglich Hardwareanforderungen (z.B. ein Kartenlesegerät für Smartcards), Sicherheit, Komplexität des Verfahrens, Handhabung durch den Benutzer (z.B. muss sich der Abonnent weder ein PIN noch ein Passwort merken) und/oder Kosten. In vielen Fällen ist eine aufwendigere Identifizierung beispielsweise eines Benutzers eines Telekommunikationsdienstes, z.B. über eine eindeutige Identifikationsnummer wie Prozessornummer, Gerätenummer, IMSI (International Mobile Subscriber Identification) oder MSISDN (Moblie Subscriber ISDN) Nummern, nicht unbedingt notwendig und/oder unter der Berücksichtigung der genannten Aspekte (z.B. Komplexität, Kosten, Handhabung) wenig sinnvoll. Der Sicherheitsstandard der vorliegenden Erfindung reicht für viele Anwendungen häufig aus. Eine weitere Verwendungsmöglichkeit der Erfindung liegt nicht nur in der einzel oder kombinierten Anwendung, sondern auch im abgestuften Anwenden des Authentifikationsverfahren mit herkömmlichen Verfahren. So könnte beispielsweise bis zu einem bestimmten, vordefinierten Geldbetrag, z. B. bei Internet-Diensten, das Authentifikationsverfahren dieser Erfindung zur Anwendung kommen, während beim Überschreiten dieses Betrages auf ein anderes Authentifikationsverfahren mit höherem Sicherheitsstandard umgestellt wird.

[0007] In einer Ausführungsvariante umfasst das Authentifikationssystem eine IVR-Schnittstelle, über welche der Abonnent aufgefordert wird, eine häufig gewählte Telefonnummer anzugeben. Einer der Vorteile dieser Ausführungsvariante ist, dass der Abonnent ausser den Eingabeelementen des Telefongeräts keine weitere Hardware für die Authentifikation benötigt.

[0008] In einer Ausführungsvariante umfasst das Authentifikationssystem ein Web-Interface des Internets, über welches der Abonnent aufgefordert wird, eine häufig gewählte Zieladresse anzugeben. Insbesondere liegen die Vorteile dieser Ausführungsvariante im graphischen, einfachen Erfassen und Bedienen der Schnittstelle durch den Benutzer.

[0009] In einer weiteren Ausführungsvariante findet die Authentifikation des Abonnenten dadurch statt, dass das Authentifikationssystem eine Liste mit mindestens einer der gespeicherten, häufig gewählten Zieladressen und mit mindestens einer beliebigen anderen Zieladresse generiert, und dass der Abonnent aus dieser Liste eine Zieladresse als häufig gewählte Zieladresse angibt. Diese Ausführungsvariante hat den Vorteil, dass, sollte sich der Abonnent nicht an eine häufig benutzte Zieladresse erinnern, ihm damit eine häufig gewählte Zieladresse zur Auswahl gegeben werden kann. Zum Beispiel ist die Aufschlüsselung der Anschlussnummer nach häufig gebrauchten Telefonnummern bei der monatlichen Gebührenrechnung für Telefonanschlüsse heute bereits gebräuchlich. Ein anderer Vorteil ist, dass die Auswahl der Zieladresse einfach und ohne manuelle Dateneingabe erfolgen kann. Dies kann insbesondere Vorteile haben bei Palmtop-Geräten oder Touch-Screens, welche beispielsweise aus hygienischen, technischen oder Kostengründen nur über eine einfache graphische Eingabe ohne Tastatur verfügen.

[0010] In einer weiteren Ausführungsvariante findet die Authentifikation des Abonnenten dadurch statt, dass der Abonnent seine Angaben mittels gesprochener Sprache über ein Kommunikationsendgerät eingibt. Die Schnittstelle zum Authentifikationssystem kann insbesondere ein Spracherkennungsmodul umfassen. Einer der Vorteile dieser Ausführungsvariante ist, dass die Authentifikation für den Abonnenten sehr einfach ist, minimale Kenntnisse der Benutzerschnittstelle voraussetzt und keine weiteren Eingabegeräte benötigt.

[0011] Es ist anzufügen, dass bei allen Ausführungsvarianten der Anbieter dem Abonnenten bei der Authentifikation optional, z.B. zum Vereinfachen des Authentifikationverfahrens, eine mögliche Abonnentenadresse, also z.B. eine Anschlussnummer eines Telefonnetzes oder eine IP-Adresse, vorschlagen kann oder z.B. mittels Anschluss- oder Netzwerkadressenerkennung die Abonnentenadresse fest vorgibt. Die Wahl der Ausführungsvariante kann insbesondere vom gewünschten Sicherheitsstandard oder der gewählten Benutzerschnittstelle abhängen. Ideale Anwendungsgebiete können beispielsweise, neben der Authentifikation beim Benutzen von Internet- und Onlinediensten, auch die Authentifikation bei Diensten sein, welche Waren über die Telefonrechnung abrechnen oder bei Diensten, für welche es schwierig ist, eine physikalische Adresse des Benutzers nachzuweisen.

[0012] Bei allen Ausführungsvarianten ist es als weitere Variante möglich, den Sicherheitsstandard des Authentifikationsverfahrens zu erhöhen, indem vom Servermodul oder vom Abonnenten zusätzlich ein Zeitintervall angegeben wird, in welchem unter einer Abonnentenadresse eine Zieladresse häufig gewählt wurde. Der Sicherheitsstandard ist dann insbesondere abhängig von der Grösse des gewählten Zeitintervals.

[0013] An dieser Stelle soll festgehalten werden, dass

sich die vorliegende Erfindung neben dem erfindungsgemässen Verfahren auch auf ein System zur Ausführung dieses Verfahrens bezieht.

[0014] Nachfolgend werden Ausführungsvarianten der vorliegenden Erfindung anhand von Beispielen beschrieben. Die Beispiele der Ausführungen werden durch folgende beigelegte Figuren illustriert:

Figur 1 zeigt ein Blockdiagramm, welches den möglichen Aufbau einer Authentifizierungseinheit und einen Abonnenten eines Telekommunikationsnetzes darstellt,

Figur 2 zeigt ein Flussdiagramm, welches eine mögliche Realisierung einer ersten Ausführungsvariante mit Abonnentenadresse und einer häufig gebrauchten Zieladresse als Erkennung beschreibt,

Figur 3 zeigt ein Flussdiagramm, welches eine mögliche Realisierung einer zweiten Ausführungsvariante mit einer Auswahlliste von mindestens einer beliebigen Zieladresse und mindestens einer häufig gebrauchten Zieladresse einer Abonnentenadresse beschreibt.

[0015] Figur 1 illustriert eine Architektur, die zur Realisierung der Erfindung verwendet werden kann. Im diesem Ausführungsbeispiel enthält das Authentifikationssystem 20 ein Servermodul 30 und eine Authentifizierungseinheit 40. Der Abonnent 10 greift über eine Benutzerschnittstelle auf das Servermodul 30 zu. Das Servermodul 30 umfasst die Schnittstelle zum Abonnenten 10 und gegebenfalls auch einen angebotenen Dienst, z.B. durch den Internetprovider. Das Servermodul 30 kann beispielsweise einen Web-Server 31, einen IVR-Server 32 und/oder einen anderen Remote-Server 3x enthalten. Das Servermodul 30 nimmt die Authentifikation des Kunden über eine Authentifizierungseinheit 40 vor, wobei die Authentifizierungseinheit 40 in diesem Fall eine Schnittstelle 45, ein Betriebsmodul 41 und eine Datenbank 42 umfasst. Die Authentifizierungseinheit 40 kann insbesondere durch einen Operator einer Telekommunikationsgesellschaft extern unterhalten werden. Über die Schnittstelle 45, beispielsweise ein API (Application Programming Interface), kann das Servermodul 30 auf die Datenbank 42 und ihre Datensätze zugreifen. Die Datenbank 42 enthält Datensätze mit den Abonnentenadressen und den zugeordneten, häufig gewählten Zieladressen. Das Betriebsmodul 41 besteht aus 2 Modulen, einem Abonnentenadressenmodul 43 und einem Auswahllistenmodul 44. Das Benutzernummermodul 43 stellt eine API-Funktion zur Verfügung, welche auf Eingabe eines Datensatzes "Abonnentenadresse/häufig gewählte Zieladresse" für diese Abonnentenadresse die Datenbank 42 nach einem solchen Datensatz durchsucht und als Antwort zurückgibt, ob der Datensatz gefunden wurde oder nicht. Die API-Funktion kann beispielsweise ein prozeduraler Aufruf der Form FUN.validate(Abonnentenadresse: string; häufig_gebrauchte_Zieladresse: string):boolean sein (FUN: Frequently Used Numbers). Das Auswahllistenmodul 44 stellt eine API-Funktion zur Verfügung, welche auf Eingabe einer Abonnentenadresse eine Liste mit mindestens einer beliebigen Zieladresse und mindestens einer häufig gewählten Zieladresse, welche der Abonnentenadresse zugeordnet ist, generiert. Die API-Funktion kann beispielsweise ein prozeduraler Aufruf der Form FUN.sample(Abonnentenadresse:string; VAR häufig_gebrauchte_Zieladresse: string) sein. Nimmt das Servermodul 30 eine Authentifikation eines Abonnenten vor, fordert es den Abonnenten auf, eine Abonnentenadresse sowie eine häufig gewählte Zieladresse einzugeben. Darauf greift das Servermodul 30 über eine API-Funktion auf das Betriebsmodul 41 und das Abonnentenadressenmodul 43 zu, welche die Datensätze nach der Kombination "Abonnentenadresse/häufig gebrauchte Zieladresse" durchsucht und den Abonnenten authentifiziert, falls der Datensatz in der Datenbank 42 vorhanden ist. War die Authentifikation erfolgreich, kann das Servermodul 30, also z.B. der Provider, dem Abonnenten 10 gegebenenfalls den Zugriff auf den Dienst freigeben. Alternativ hat das Servermodul 30 die Möglichkeit, vom Abonnenten 10 nur die Eingabe einer Abonnentenadresse zu fordern. Das Servermodul 30 greift darauf über eine API-Funktion auf das Betriebsmodul 41 und das Auswahllistenmodul 44 zu, welches ihm eine Liste mit mehreren beliebigen Zieladressen und mindestens einer häufig gewählten Zieladresse generiert. Das Servermodul 30 fordert den Abonnenten 10 auf, aus dieser Liste die häufig gewählte Zieladresse auszuwählen und überprüft mittels des Abonnentenadressenmoduls 43 die Authentizität des Abonnenten 10 wie in der vorhergehenden Variante.

[0016] Figur 2 illustriert mittels eines Flussdiagramms ein erstes Ausführungsbeispiel, bei welchem das Abonnentenadressenmodul 43 (Figur 1) verwendet wird. Es ist für den Zugriff übers Telefon (z.B. IVR, SMS) oder einem Web-Interface geeignet, kann aber allgemein verwendet werden. Ein Abonnent 10 möchte z.B. einen bestimmten Dienst in Anspruch nehmen. Er beginnt deshalb mit Schritt 1 eine Serveranfrage bei dem Anbieter dieses Dienstes. In Schritt 2 verlangt das Servermodul 30 vom Abonnent 10 eine Abonnentenadresse (aln). Das kann z.B. die Anschlussnummer oder die Netzadresse sein, welche zur Verrechnung der Kosten für die Beanspruchung des Dienstes verwendet wird oder eine andere Abonnentenadresse. Das Servermodul 30 kann optional, z.B. durch Anschlusserkennung oder Netzwerkadressenerkennung, dem Abonnenten 10 eine Default-Abonnentenadresse vorschlagen. In Schritt 3 verlangt das Servermodul 30 vom Abonnenten 10 eine Zieladresse (sample), von welcher der Abonnent 10 weiss, dass er sie in letzter Zeit häufig benutzt hat. Bei graphischen Benutzerschnittstellen können Schritt 2 und 3 kombiniert werden. Beim Zugriff über Telefon wird der Abonnent 10 über einen IVR-Server 32

aufgefordert, die häufig gebrauchte Zieladresse, z.B. eine Telefonnummer oder eine IP-Nummer einzutippen. In Schritt 4 ruft das Servermodul 30 mit dem Datensatz "aln/sample" die API-Funktion (FUN.validate) auf, welche den Zugriff auf das Abonnentenadressenmodul 43 erlaubt. Die Authentifizierungseinheit 40 überprüft, ob der Datensatz "aln/sample" in der Datenbank 42 vorhanden ist (Schritt 5). Kann der Datensatz nicht gefunden werden, handelt es sich um keinen autorisierten Abonnenten 10 und/oder eine der Zieladressen wurde vom Abonnenten 10 falsch eingegeben (Schritt 6). Der Prozess kann in diesem Fall z.B. bei Schritt 2 oder Schritt 3 fortfahren, indem das Servermodul 30 den Abonnenten 10 auffordert, nochmals die Zieladresse(n) einzugeben. Wird der Datensatz gefunden, erhält das Servermodul 30 die Nachricht, dass der Abonnent 10 authentifiziert wurde und das Servermodul 30, z.B. der Provider, kann dem Abonnenten den Zugriff auf den Dienst freigeben (Schritt 7).

[0017] Figur 3 illustiert mittels eines Flussdiagramms ein zweites Ausführungsbeispiel, bei welchem das Auswahllistenmodul 44 (Figur 1) verwendet wird. Es eignet sich insbesondere für ein Web-Interface, kann aber auch bei anderen Benutzerschnittstellen verwendet werden. Schritt 1 und 2 sind analog wie bei Figur 2. In Schritt 3 ruft das Servermodul 30 mit der Abonnentenadresse (aln) die API-Funktion (FUN.sample) auf, welche den Zugriff auf das Auswahllistenmodul 44 erlaubt. Die Authentifizierungseinheit 40 überprüft in Schritt 4, ob ein Datensatz für diese Abonnentenadresse vorhanden ist. Ist kein Datensatz vorhanden, kann z.B. das Servermodul 30 den Abonnenten 10 mit Schritt 2 zur nochmaligen Eingabe einer Abonnentenadresse auffordern. Wird für diese Abonnentenadresse ein Datensatz gefunden, generiert in Schritt 5 die Authentifizierungseinheit 40 eine Liste mit mindestens einer beliebigen Zieladresse und mindestens einer häufig gewählten Zieladresse für die Abonnentenadresse und gibt diese Liste an das Servermodul 30 zurück. In Schritt 6 fordert das Servermodul 30 den Abonnenten 10 auf, aus der Liste die häufig gewählte Zieladresse (sample) auszuwählen. In Schritt 7 ruft das Servermodul 30 mit dem Datensatz "aln/sample" die API-Funktion (FUN.validate) auf, welche den Zugriff auf das Abonnentenadressenmodul 43 erlaubt. Die Authentifizierungseinheit 40 überprüft, ob der Datensatz "aln/sample" in der Datenbank 42 vorhanden ist (Schritt 8). Kann der Datensatz nicht gefunden werden, handelt es sich um keinen autorisierten Abonnenten 10 und/oder eine der Zieladressen wurde vom Abonnenten 10 falsch eingegeben (Schritt 9). Der Prozess kann z.B. bei Schritt 3 nochmals beginnen, indem das Servermodul 30 sich eine neue Auswahlliste generieren lässt. Wird der Datensatz gefunden, erhält das Servermodul 30 die Nachricht, dass der Abonnent 10 authentifiziert wurde und das Servermodul 30, z.B. der Provider, kann dem Abonnent 10 den Zugriff auf den Dienst freigeben (Schritt 10).

Patentansprüche

1. Verfahren zur Authentifikation eines Abonnenten eines Telekommunikationsnetzes, dadurch gekennzeichnet,

   dass der Abonnent (10) mindestens eine der über eine Abonnentenadresse des Telekommunikationsnetzes häufig gewählten Zieladresse einem Authentifikationssystem (20) angibt und

   dass das Authentifikationssystem (20) die angegebene Zieladresse mit häufig gewählten Zieladressen vergleicht, die der Abonnentenadresse zugeordnet abgespeichert sind.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Abonnent (10) ein Benutzer eines Telefonnetzes ist, welcher mindestens eine der über eine Anschlussnummer des Telefonnetzes häufig gewählten Telefonnummern einem Authentifikationssystem (20) angibt und dass das Authentifikationssystem (20) die angegebene Telefonnummer mit häufig gewählten Telefonnummern vergleicht, die der Anschlussnummer zugeordnet abgespeichert sind.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Abonnent (10) ein Benutzer eines IP-Netzes ist, welcher mindestens eine der über eine IP-Adresse des Abonnenten des IP-Netzes häufig gewählten IP-Nummern einem Authentifikationssystem (20) angibt und dass das Authentifikationssystem (20) die angegebene IP-Nummer mit häufig gewählten IP-Nummern vergleicht, die der IP-Adresse des Abonnenten zugeordnet abgespeichert sind.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Abonnent eines Telekommunikationsnetzes (10) durch das Authentifikationssystem (20) über eine IVR-Schnittstelle (32) aufgefordert wird, eine häufig gewählte Zieladresse anzugeben.

5. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Abonnent eines Telekommunikationsnetzes (10) die häufig gewählte Zieladresse dem Authentifikationssystem (20) über ein Web-Interface des Internets angibt.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das Authentifikationssystem (20) eine Liste mit mindestens einer der gespeicherten, häufig gewählten Zieladressen und mit mindestens einer beliebigen anderen Zieladresse generiert, und dass der Benutzer (10) aus dieser

Liste eine Zieladresse als häufig gewählte Zieladresse angibt.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Abonnent eines Telekommunikationsnetzes (10) seine Angaben mittels gesprochener Sprache über ein Kommunikationsendgerät eingibt.

8. System zur Authentifikation von Abonnenten (1) eines Telekommunikationsnetzes, dadurch gekennzeichnet,

dass es ein Servermodul (30) umfasst, welches vom Benutzer eines Telekommunikationsnetzes mindestens eine der über eine Abonnentenadresse des Telekommunikationsnetzes häufig gewählten Zieladressen verlangt und

dass es eine Authentifizierungseinheit (40) umfasst, welche die angegebene Zieladresse zur Authentifikation mit den häufig gewählten Zieladressen vergleicht, die der Abonnentenadresse zugeordnet sind.

9. System zur Authentifikation nach Anspruch 8, dadurch gekennzeichnet, dass der Abonnent (10) ein Benutzer eines Telefonnetzes ist, dass die Abonnentenadresse eine Anschlussnummer dieses Telefonnetzes ist und dass die häufig gewählten Zieladressen häufig gewählte Telefonnummern sind.

10. System zur Authentifikation nach Anspruch 8, dadurch gekennzeichnet, dass der Abonnent (10) ein Benutzer eines IP-Netzes ist, dass die Abonnentenadresse eine IP-Nummer ist und dass die häufig gewählten Zieladressen häufig gewählte IP-Nummern sind.

11. System zur Authentifikation nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass das Servermodul (30) einen IVR-Server (32) umfasst, welcher vom Benutzer die Abonnentenadresse und die häufig gewählte Zieladresse anfordert und entgegennimmt.

12. System zur Authentifikation nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass das Servermodul (30) einen Web-Server (31) umfasst, welcher vom Benutzer die Abonnentenadresse und die häufig gewählte Zieladresse über ein Web-Interface anfordert und entgegennimmt.

13. System zur Authentifikation nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass die Authentifizierungseinheit (40) ein Auswahllistenmodul (44) umfasst, welches eine Liste mit mindestens einer der gespeicherten, häufig gewählten Zieladressen und mit mindestens einer beliebigen anderen Zieladresse generiert, aus welcher Liste der Benutzer (10) eine Zieladresse als häufig gewählte Zieladresse angibt.

14. System zur Authentifikation nach einem der Ansprüche 8 bis 13, dadurch gekennzeichnet, dass das Servermodul (30) eine Benutzerschnittstelle umfasst, welche die Angaben des Benutzers in gesprochener Sprache entgegennimmt.

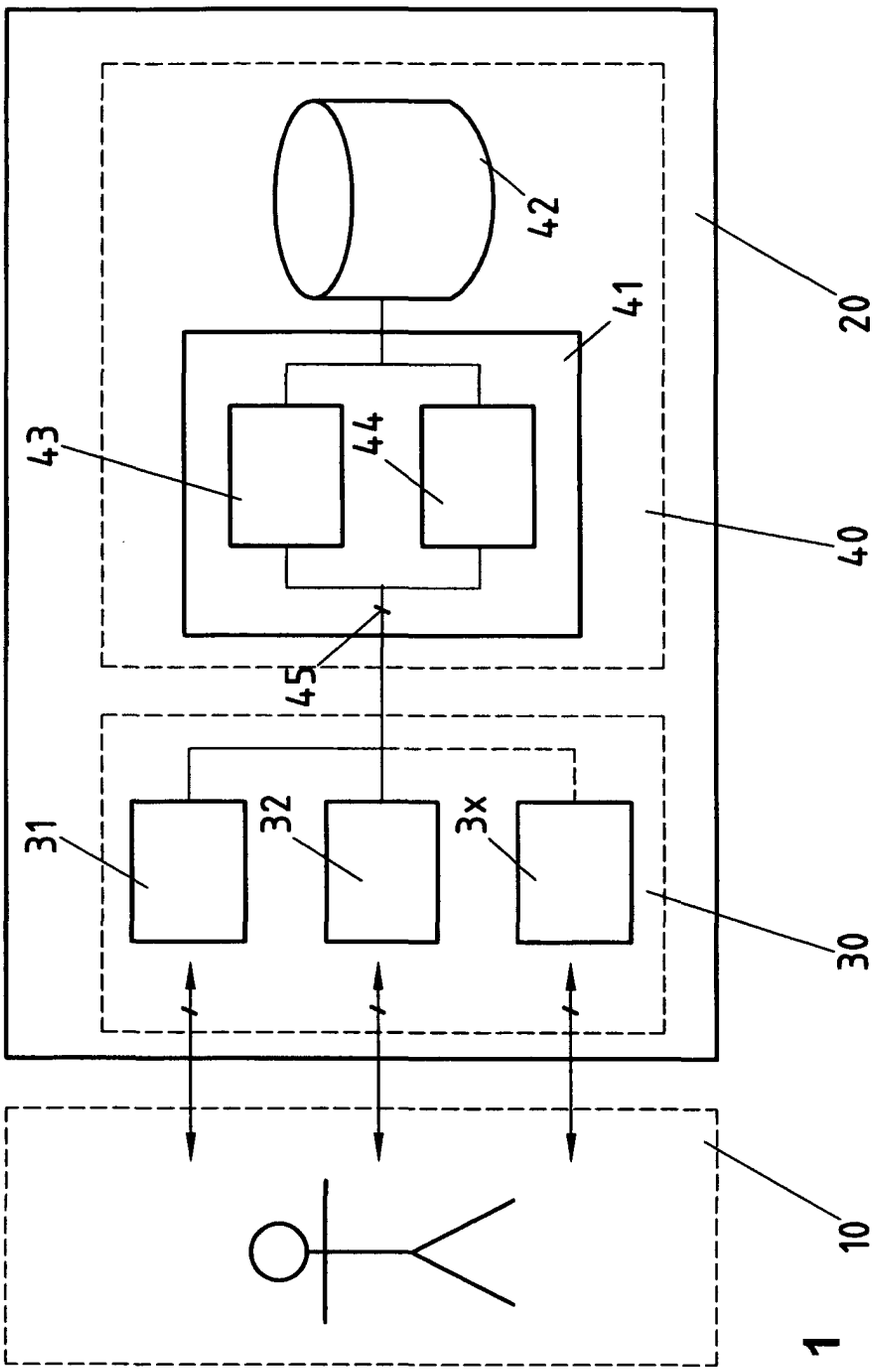

FIG. 1

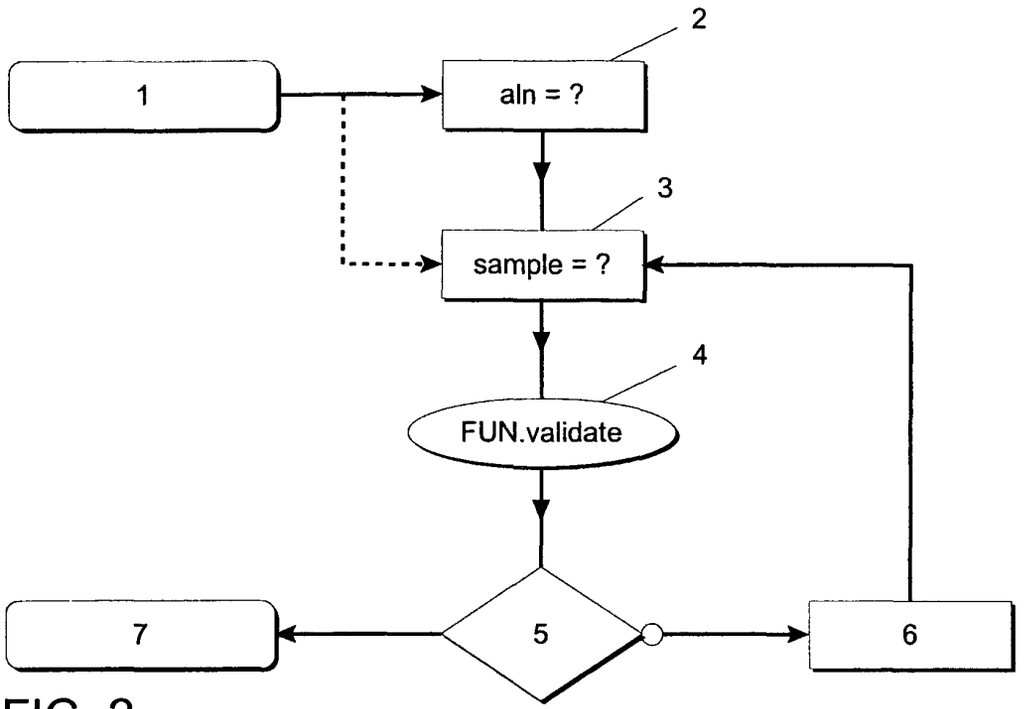
1
aln = ?
2
sample = ?
3
FUN.validate
4
5
6
7

FIG. 2

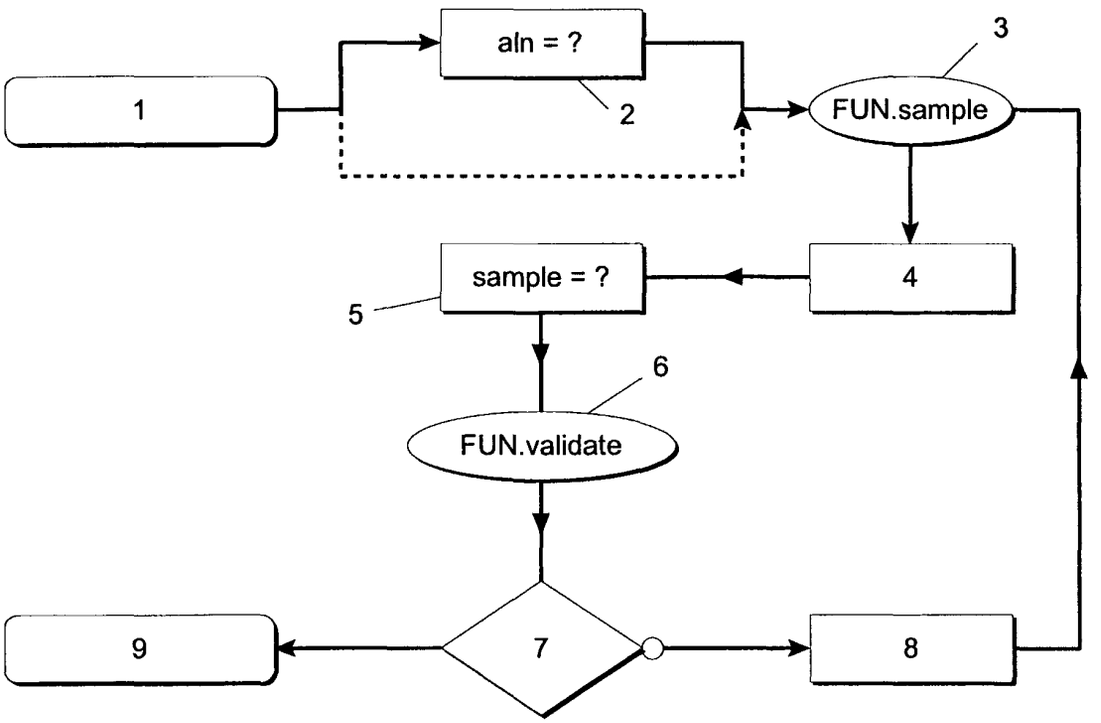
1
aln = ?
2
FUN.sample
3
sample = ?
4
5
FUN.validate
6
7
8
9

FIG. 3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 81 0008

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
A	US 5 633 914 A (ROSA STEPHEN P) 27. Mai 1997 (1997-05-27) * Spalte 3, Zeile 60 - Spalte 4, Zeile 18 *	1,2,8,9	H04M3/38 H04L29/06 G06F1/00
A	EP 0 756 410 A (SIEMENS AG) 29. Januar 1997 (1997-01-29) * Zusammenfassung *	1,2,8,9	
A	US 5 774 525 A (YUNG MARCEL MORDECHAY ET AL) 30. Juni 1998 (1998-06-30) * Zusammenfassung *	1,2,8,9	

RECHERCHIERTE SACHGEBIETE (Int.Cl.7)

H04M
H04L
H04Q
G06F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	20. Juni 2000	Cremer, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie,übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 00 81 0008

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

20-06-2000

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5633914 A	27-05-1997	CA 2230030 A	06-03-1997
		WO 9708907 A	06-03-1997
		US 5918173 A	29-06-1999
EP 0756410 A	29-01-1997	DE 19527022 A	30-01-1997
US 5774525 A	30-06-1998	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82